



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/877,655	06/08/2001	Hovav Shacham	36321.8007.US	9498

22918 7590 01/23/2006

PERKINS COIE LLP
P.O. BOX 2168
MENLO PARK, CA 94026

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 01/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/877,655	Applicant(s) SHACHAM ET AL.	
	Examiner Michael J. Simitoski	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 November 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 33-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 33-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 11/18/2005 was received and considered.
2. Claims 33-40 are pending.

Response to Arguments

3. Applicant's arguments with respect to the previously-presented claims have been considered but are moot in view of the new ground(s) of rejection.

Drawings

4. The drawings are objected to because Fig. 2 (#235, #240) recites “e¹” where it should recite “e’”. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will

be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

5. Claims 33-36 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claims 33-36, claim 33 recites “generating prime numbers r_1 and r_2 , generating N by multiplying r_1 and r_2 , selecting arbitrary numbers p and q”, however the specification (Fig. 2) discloses “generating prime numbers p and q, generating N by multiplying p and q, selecting arbitrary numbers r_1 and r_2 .” For the purposes of this Office Action, the claim is understood to read “generating prime numbers p and q, generating N by multiplying p and q, selecting arbitrary numbers r_1 and r_2 .”

Regarding claims 33-36, claim 33 recites “calculating e' by multiplying d^{-1} and $\text{mod}\varphi(N)$ ”, however the modulo operation is not a multiplicand. For the purposes of this Office Action, this limitation is understood to read “calculating e' by performing $d^{-1} \text{mod}\varphi(N)$ ”.

Regarding claims 33-36, claim 33 recites “ $\text{mod}\varphi(N)$ ”, however the symbol $\varphi(N)$ is indefinite. This could be corrected by stating “ $\varphi(N)$, where $\varphi(N)$ represents ...”.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Network Security Essentials: Applications and Standards by Stallings in view of Handbook of Applied Cryptography by Menezes et al. (**Menezes**) and “Homework 4 with Extensive Hints” by **Immerman**.

Regarding claims 33-34, Stallings discloses coupling a client to a web server (p. 214, Fig. 7.6), using a public key to encrypt a pre-master secret R such that the encrypted pre-master secret R is a secret encrypted C , at the client (p. 217, ¶3), sending the secret encrypted C to the web server from the client (p. 217, ¶3), receiving the secret encrypted C at the web server, decrypting the secret encrypted C to obtain the encrypted pre-master secret R at the web server (p. 218, ¶5) and using the encrypted pre-master secret R to establish a session encryption key (p. 208, last paragraph). Menezes teaches standard RSA parameter generation, wherein (n, e) is the public key with $n=pq$ (§8.2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate N , the product of two distinct primes, p and q . One of ordinary skill in the art would have been motivated to perform such a modification to use the RSA public key encryption/decryption function, as taught by Menezes (§8.2.1). Menezes further teaches that $x^d \bmod n$ (decryption) can be more efficiently computed using the pair $x^{d_p} \bmod p$ and $x^{d_q} \bmod q$ where $d_p = d \bmod p-1$ and $d_q = d \bmod q-1$

Art Unit: 2134

(generating two numbers $\langle d_p, d_q \rangle$), by then recombining the solution using the CRT/Garner's algorithm (§14.5.2, 14.75 Note). Further, Immerman teaches that using the Chinese Remainder Theorem, integers mod ab ($z = \text{int}(\text{mod } ab)$) can be written in terms of integers mod a ($x = \text{int}(\text{mod } a)$) and mod b ($y = \text{int}(\text{mod } b)$), such that $z \equiv x(\text{mod } a)$ and $z \equiv y(\text{mod } b)$ (page 1, §Chinese Remainder Theorem). As such, by the Chinese Remainder Theorem, $d_p = d(\text{mod } p - 1)$ and $d_q = d(\text{mod } q - 1)$ share the relationship $d = d_p(\text{mod } p - 1)$ and $d = d_q(\text{mod } q - 1)$, the decryption pair being $\langle d_p, d_q \rangle$ (p. 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Stallings, as modified above, to select two numbers r_1 and r_2 (d_p, d_q) and generate d (decryption key) such that $d = r_1(\text{mod } p - 1)$ and also $d = r_2(\text{mod } q - 1)$, whereby e' is calculated by $d^{-1} \text{mod } \phi(N)$ (as this is the relationship d and e must have, according to Menezes, §8.2.1) and whereby the public key is $[N, e']$ and the private key is $[r_1, r_2]$. One of ordinary skill in the art would have been motivated to perform such a modification to more efficiently compute decryption, as taught by Menezes (§14.5.2, 14.75 Note) and Immerman (p. 1).

Regarding claims 35-36, Stallings discloses TLS (p. 219) and IPSec (p. 163).

8. Claims 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Network Security Essentials: Applications and Standards by Stallings in view of Handbook of Applied Cryptography by Menezes et al. (Menezes).

Regarding claims 37-38, Stallings discloses coupling a client to a web server (p. 214, Fig. 7.6), using a public key to encrypt a pre-master secret R such that the encrypted pre-master secret

Art Unit: 2134

R is a secret encrypted C, at the client (p. 217, ¶3), sending the secret encrypted C to the web server from the client (p. 217, ¶3), receiving the secret encrypted C at the web server, decrypting the secret encrypted C to obtain the encrypted pre-master secret R at the web server (p. 218, ¶5) and using the encrypted pre-master secret R to establish a session encryption key (p. 208, last paragraph). Stallings lacks generating a public/private key pair at the web server based upon a selection of a pair of prime numbers and a pair of arbitrarily selected numbers. However, Menezes teaches the RSA public key algorithm, where a public key is generated using two prime numbers, p and q and a pair of arbitrarily selected numbers, e and ϕ (¶8.2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the public/private key pair at the web server based upon a selection of a pair of prime numbers and a pair of arbitrarily selected numbers. One of ordinary skill in the art would have been motivated to perform such a modification to use the RSA public key encryption/decryption function, as taught by Menezes (¶8.2.1).

Regarding claims 39-40, Stallings discloses TLS (p. 219) and IPSec (p. 163).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Art Unit: 2134

Any response to this action should be mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:


(571) 273-8300
(for formal communications intended for entry)

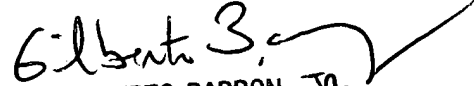
Or:

(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


MJS
January 17, 2006


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100